JUST WHAT THE DOCTOR ORDERED?

SCOTT ERVEN
Founder/President – SecMedic
@scotterven

SHAWN MERDINGER
Healthcare Security Researcher
Founder – MedSec LinkedIn Group
@medseclinkedin

Why Research Medical Devices?

- Patient Safety & Quality Patient Care
- To Equip Defenders In Assessing & Protecting These Life Saving Devices
- Directly Contributes To & Affects Healthcare Organizations' Mission and Values

Disclosure Process Overview

- April 30th – SMB Findings Disclosed To DHS/ICS-CERT
- May 5th – SMB Detailed Briefing With DHS/ICS-CERT
- May 20th – Additional Disclosure To DHS/ICS-CERT for Defibs, Healthcare Orgs
- Ongoing Assistance Provided To Federal Agencies, Healthcare Organizations and Manufacturers

What Will Be Revealed?

- No Zero Days
- Most Vulnerabilities Not From This Decade
- Threat Modeling – Connecting The Dots
- Medical Device Exposure From Public Internet

Bad News

- The external findings pose a significant risk to patient safety and medical devices
- We located most of these external risks within 1 hour utilizing only previously disclosed vulnerabilities and open source reconnaissance
- These findings provide support that Healthcare is 10 years behind other industries in addressing security

Good News

- These significant external risks can be mitigated easily
- The external risks can be identified by an organization within 1 hour using open source reconnaissance tools
- The external findings can be remediated with little to no investment from an organization

Review of Previous Research

- Lab Systems
- Refrigeration Storage
- PACS – Imaging
- MRI/CT
- Implantable Cardiac Defibrillators
- External Cardiac Defibrillators
- Infusion Pumps
- Medical Device Integration

Review of Previous Research - Top Risks

- Hard-Coded Privileged Accounts
- Unencrypted Web Applications & Web Services/Interfaces
- Excessive Services With No Operational Use Case
- System Updates & Patching

Phase II Research – Why Do More?

- Many have been misinformed that medical devices can not be accessed by an attacker from the Internet.
  - "The biggest vulnerability was the perception of IT health care professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise." – FBI Advisory April 8th, 2014 PIN#140408-009
- Physicians and public are unaware or have been misinformed about the risks associated with these life saving devices.

Phase II Research – Why Do More?

- “I have never seen an industry with more gaping holes. If our financial industry regarded security the way the health-care sector does, I would stuff my cash in a mattress under my bed.”
  - Avi Rubin, John Hopkins University 2012/12/25

Shodan Search & Initial Finding

- Doing a search for anesthesia in Shodan and realized it was not an anesthesia workstation.
- Realized it was a public facing system with SMB open, and it was leaking intelligence about the healthcare organization's entire network including medical devices.

Initial Healthcare Organization Discovery

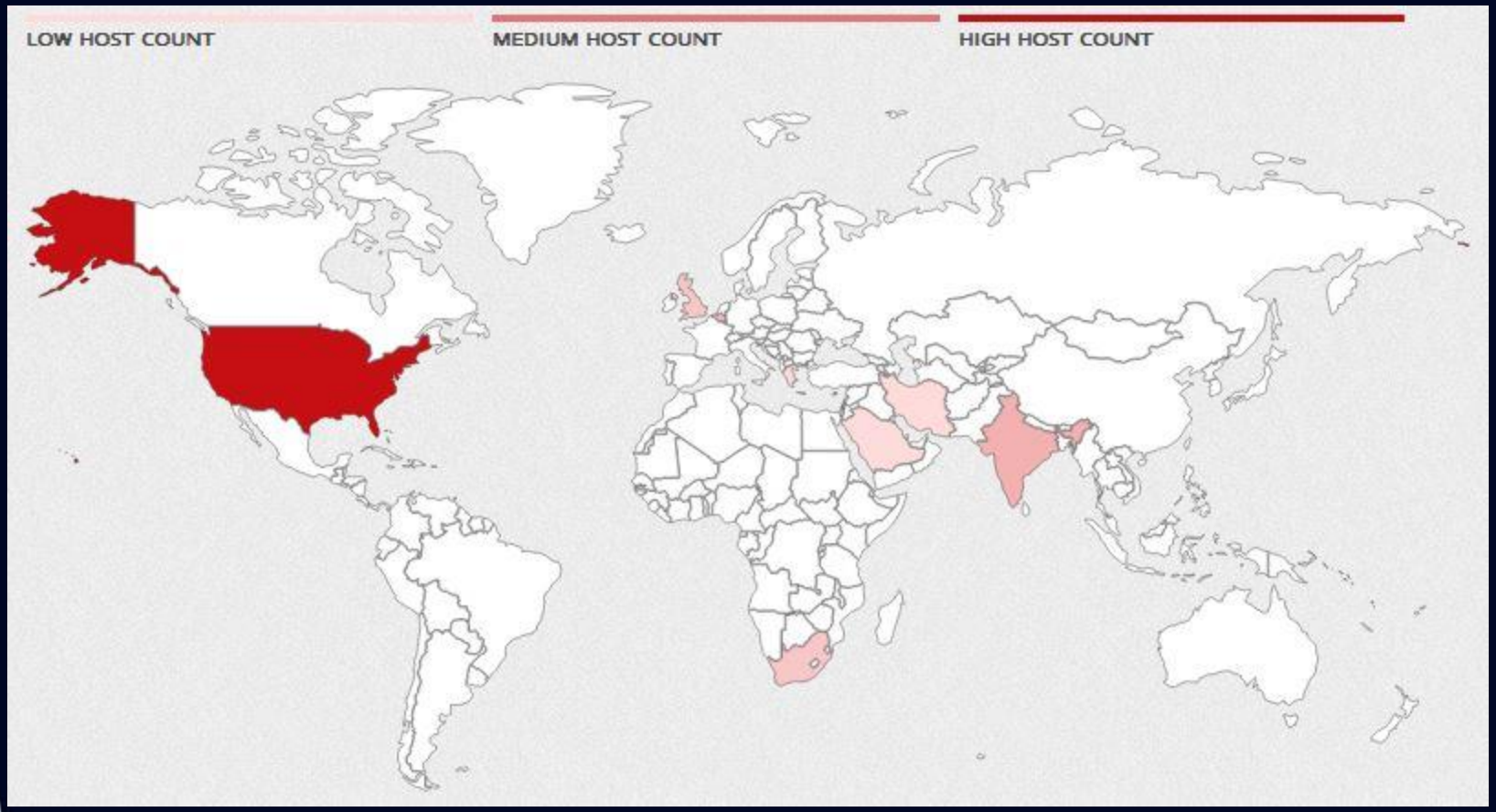
- Very large US healthcare system consisting of over 12,000 employees and over 3,000 physicians. Including large cardiovascular and neuroscience institutions.
- Exposed intelligence on over 68,000 systems and provided direct attack vector to the systems.
- Exposed numerous connected third-party organizations and healthcare systems.

So Did We Only Find One?

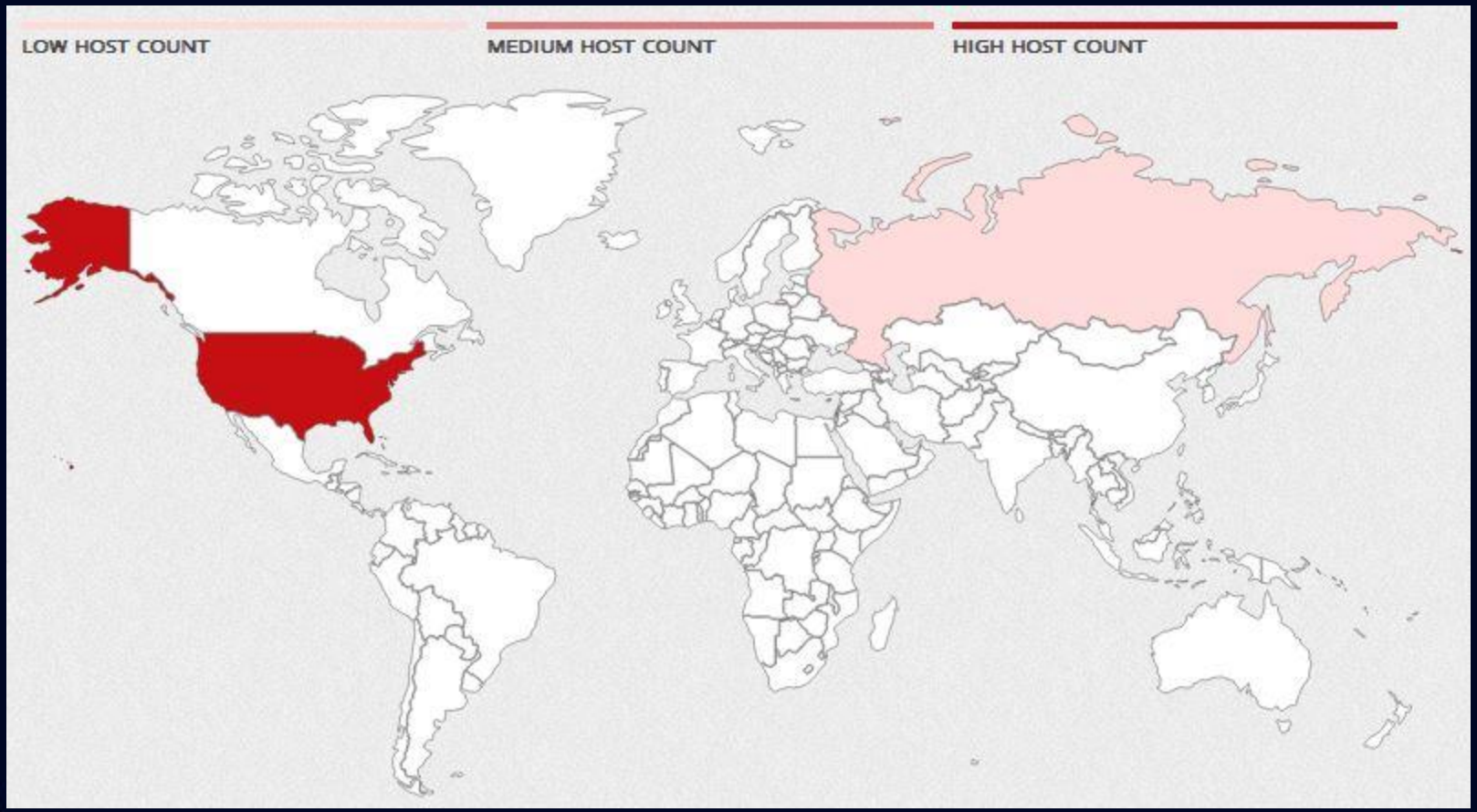
- Of Course Not. We Found Hundreds!!

- Change the search term and many more come up. Potentially thousands if you include exposed third-party healthcare systems.

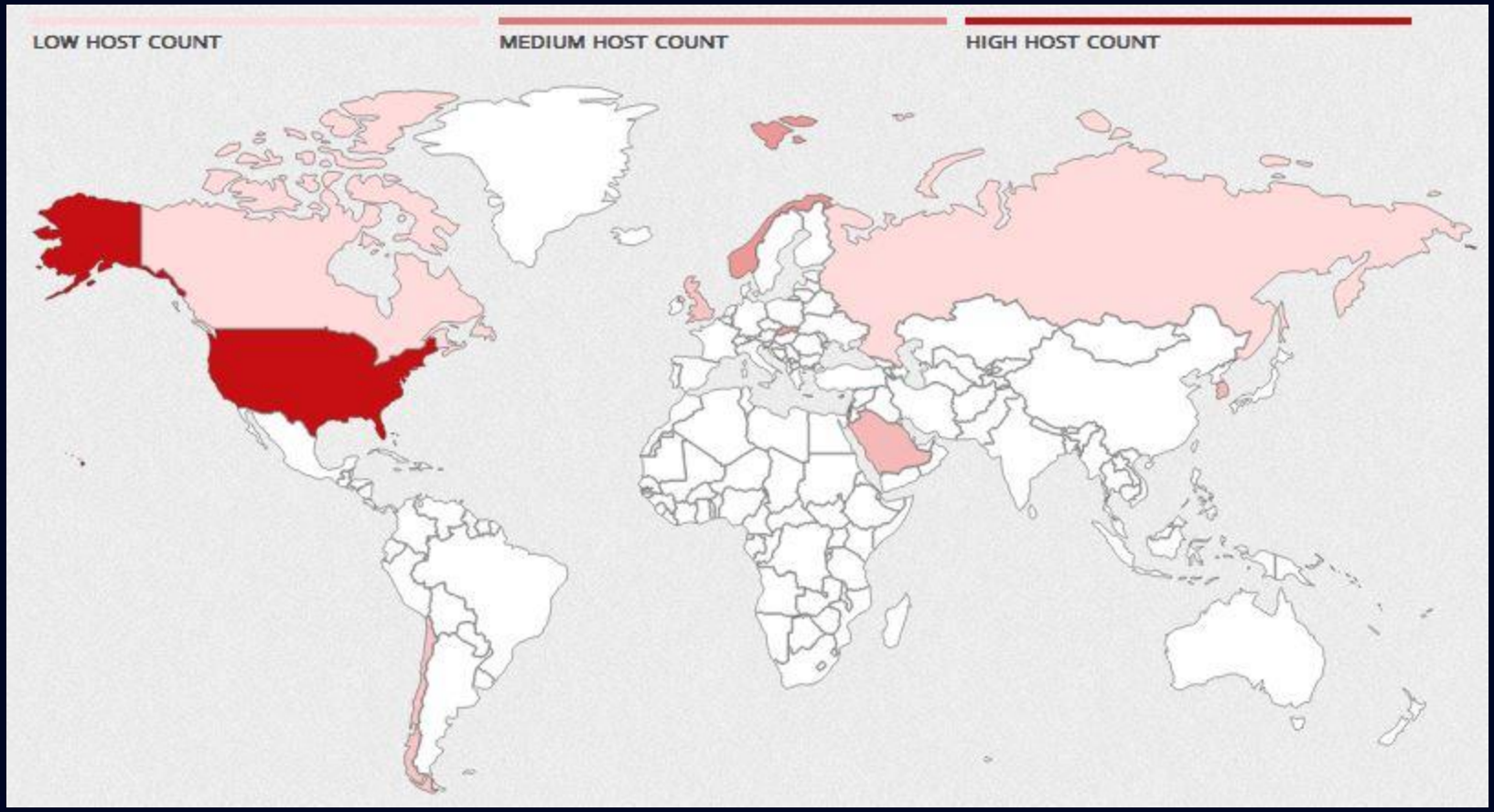
Heat Map – Health*



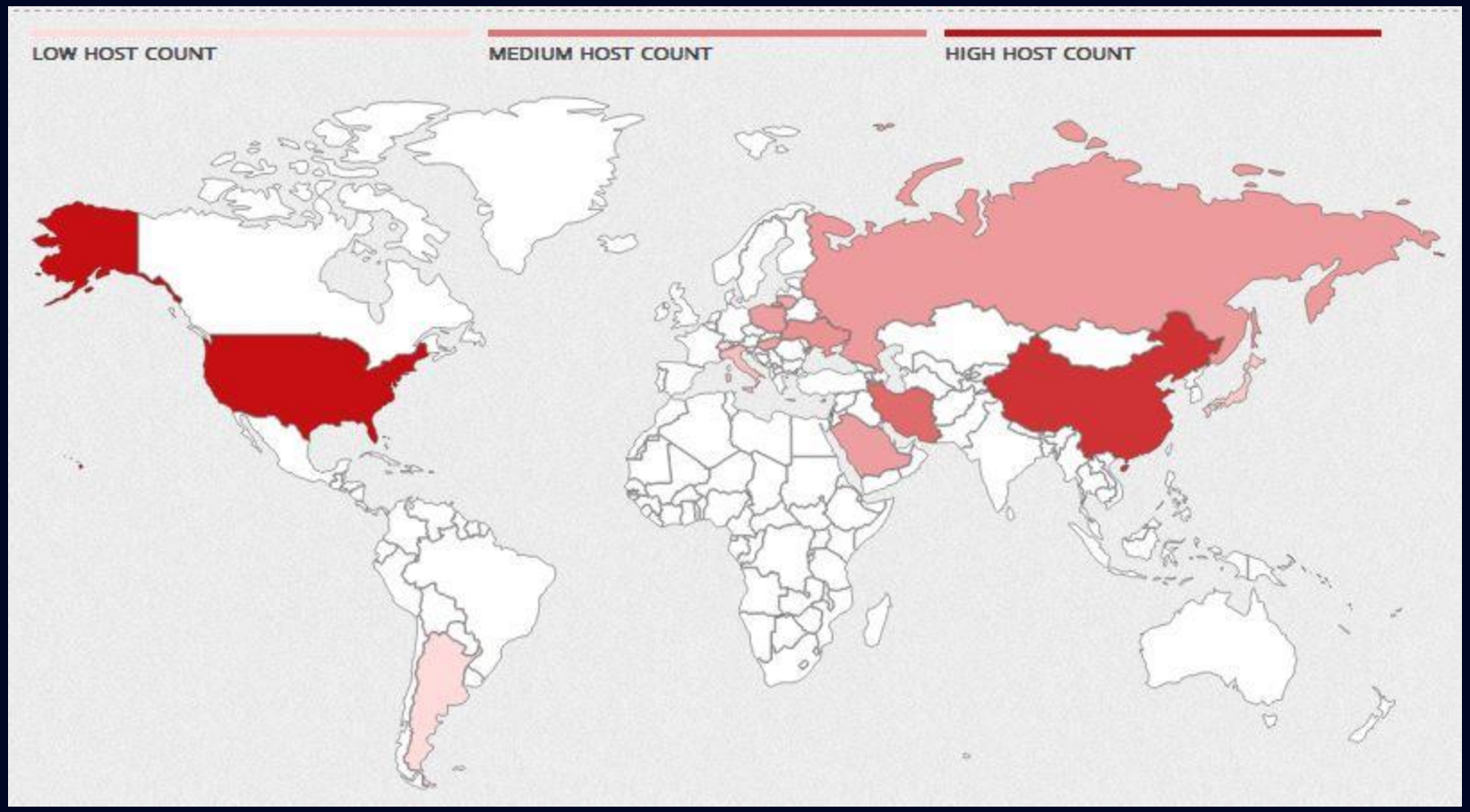
Heat Map - Clinic



Heat Map - Hospital

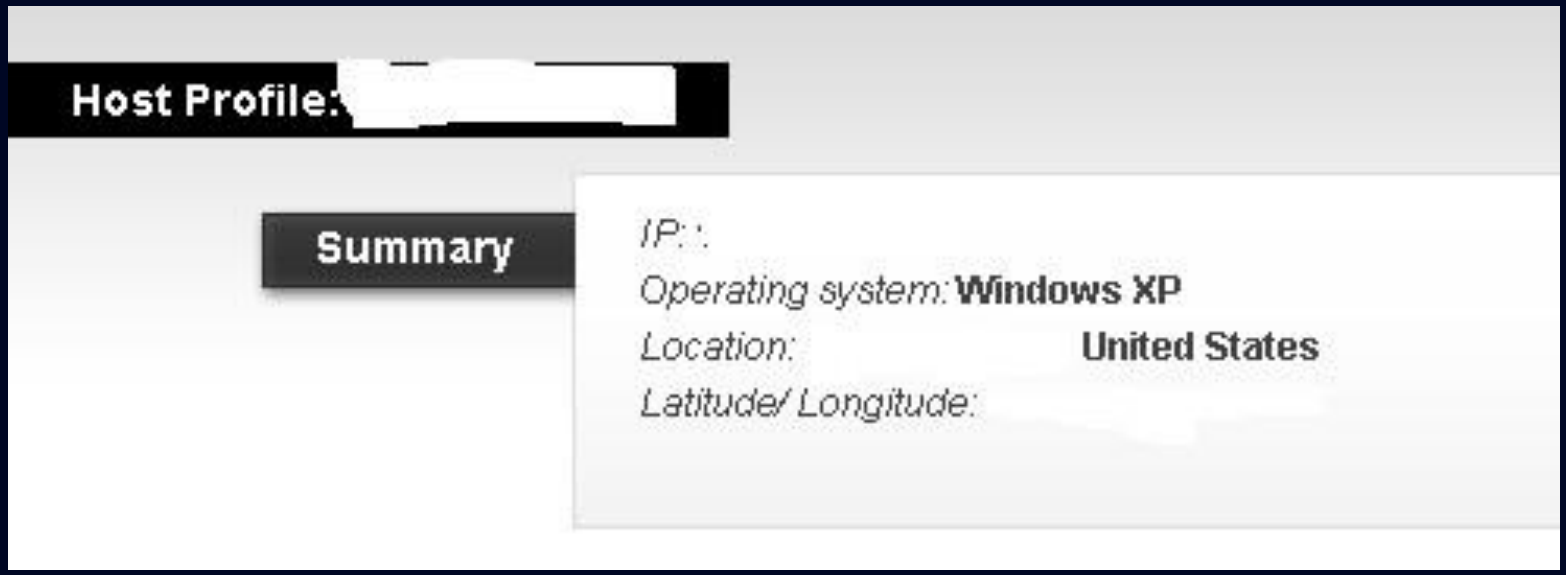


Heat Map - Medical



So Who Cares About SMB Right?

- Well it also happened to be a Windows XP system vulnerable to MS08-067 in many instances!! CVE-2008-4250



Why Does This Matter?

- It’s A Goldmine For Adversaries & Attackers!!
- It leaks specific information to identify medical devices and their supporting technology systems and applications.
- It leaks system hostnames on connected devices in the network.
- It often times leaks floor, office, physician name and also system timeout exemptions.

Let Me Paint The Picture.

System with Lockout Exemption:

```
050580      Echo Vas OR 1 -   _ScreenLock_0_Exception
050581   _ScreenLock_0_Exception
050583       OR 1-   _ScreenLock_0_Exception
050585    Echo Vas OR 2 -   _ScreenLock_0_Exception
```

Impact:
System May Not Require Login

EMR:

```
EP03 EPIC Cogito Clarity RDBMs Server
EP04 EPIC Clarity Test Console
EP05 EPIC Business Objects test
EP06 EPIC Realy BCA Server 1
EP07 EPIC Hyperspace
EP08 EPIC Hyperspace Web Server 1
EP09 EPIC Hyperspace Web Server 2
EP10 EPIC Hyperspace Web Server 3
EP11 EPIC Web BLOB Server
EP12 EPIC Kuiper Server
EP13 EPIC EPS Server 1
EP14 EPIC EPS Server 2
EP15 EPIC Interconnect
EP16 EPIC Care Everywhere
EP17 EPIC Soap Proxy
EP18 EPIC System Pluse
EP19 EPIC Multipurpose SQL Server
EP20 EPIC - Citrix XenApp 6.5 License/Web
EP21 EPIC - Citrix XenApp 6.5 Application Server
EP22 EPIC - Citrix XenApp 6.5 Application Server/DC
EP23 EPIC My Chart
EP24 EPIC Care Link
EP25 EPIC File Service
```

Impact:
Electronic Medical Record Systems

Getting a little warmer!!

```
W064959 PACS Room 1 Radiology SSO Screenlock Exception
W064960
W064967 PACS MRI SSO Screenlock Exception.
W064970
W064971
W064974 PACS CT3              SSO Screenlock Exception
```

Impact: PACS Imaging Systems, MRI/CT Systems

```
073447      1- Telemetry
073464      1 Telementry
073472      1 telementry
```

Impact: Infant Abduction Systems

This Is Not Good.

Cardiology Systems:

```
060768          1 - Dr.
060911          D, Dr. C      , Cath Lab Admin
061463          C - Cardiac Core Lab
063012          C - EP -
064320 Adrienne C           - Cardiovascular Lab
065772          c pacemaker
```

```
W069454 Gor     first floor Peds Nuclear Medicine
```

```
046142 Anestisia OR
046774
046785 Me     A
046798
046799 Da     Fau
047271 Anesthesia Work Room
```

Impact:
Pacemaker Controller Systems
Pediatric Nuclear Medicine
Anesthesia Systems

OK You Found A Few Devices Right?

- Wrong!!
- We dumped the raw data on the organization and extracted the following information on medical devices and their supporting systems.
- We identified thousands of medical devices and their supporting systems inside this organization.

Summary Of Devices Inside Organization

- Anesthesia Systems – 21
- Cardiology Systems – 488
- Infusion Systems – 133
- MRI – 97
- PACS Systems – 323
- Nuclear Medicine Systems – 67
- Pacemaker Systems - 31

Potential Attacks – Physical Attack

- We know what type of systems and medical devices are inside the organization.
- We know the healthcare organization and location.
- We know the floor and office number
- We know if it has a lockout exemption

Potential Attacks – Phishing Attack

- We know what type of systems and medical devices are inside the organization.
- We know the healthcare organization and employee names.
- We know the hostname of all these devices.
- We can create a custom payload to only target medical devices and systems with known vulnerabilities.

Potential Attacks – Pivot Attack

- We know the direct public Internet facing system is vulnerable to MS08-067 and is Windows XP.
- We know it is touching the backend networks because it is leaking all the systems it is connected to.
- We can create a custom payload to pivot to only targeted medical devices and systems with known vulnerabilities.

Potential Attacks – Targeted Attack

- We can use any of the previous three attack vectors.
- We now know their Electronic Medical Record system and server names to attack and gain unauthorized access. This can tell an attacker where a patient will be and when.
- We can launch a targeted attack at a specific location since we know specific rooms these devices are located in.

Disclosure Overview & Results – Big Win!

- DHS/ICS-CERT Coordinated Disclosure
- DHS/ICS-CERT Coordinated Follow-Up Call With Affected Organization
- Affected Organization Shared Incident Response Documentation
- First Time DHS/ICS-CERT Had Coordinated Security Researchers & Healthcare Organization

Are Medical Devices On Public Internet?

- Yes They Are
- In Many Cases It Is By Design
- In Many Cases They Utilize Public Cellular Carrier Networks

So Did We Find Anything Public Facing?

- Defibrillators
- Fetal/Infant Monitoring Systems
- EEG Systems
- PACS/Imaging Systems

What Else Was Accessible?

- Healthcare Systems
  - Unauthenticated Edge Routers
- Device Manufacturer Infrastructure
- Third-Party Contracted Organizations

Case Study – Glucose Meters

- 1st Reported Medical Device On Public IP
  - Late 2012
- Roche Glucose Meter
  - Basestation Has Telnet Open
- Excellent Vendor Response
- Excellent DHS/ICS-CERT Response

Case Study – Kodak PACS Systems

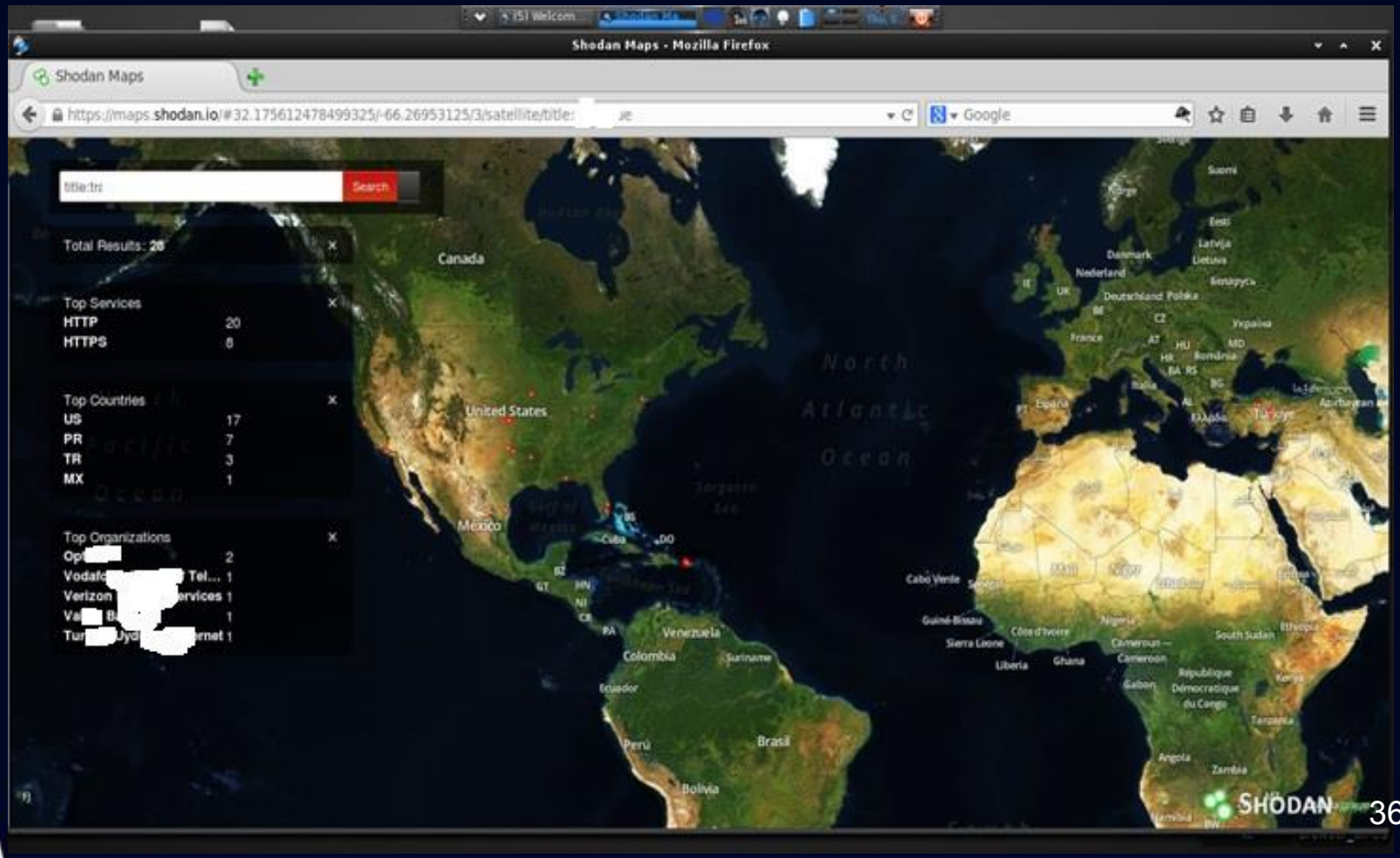
- Hundreds Sitting On Public IP
- Issues
  - Client Connectivity Requires Old Browser
  - Internet Explorer 6.0
- Dedicated Client Box Only For This?

Case Study – Fetal Monitors

- May 18th – Fetal Monitor Findings Disclosed To DHS/ICS-CERT, Manufacturer, FDA, OCR, Joint Commission
- Previous Disclosure
  - Dec. 2012 - Fetal monitor findings reported to DHS ICS-CERT
  - Media Coverage
    - 3/25/2013
      - http://www.wired.com/2013/03/our-health-information/
    - 9/5/2013
      - http://www.forbes.com/sites/kashmirhill/2013/09/05/the-crazy-things-a-savvy-shodan-searcher-can-find-exposed-on-the-internet/

Case Study – 28 Fetal Monitors

- Shodan Map Of Fetal Monitors On Public IP



Case Study – Fetal Monitors

- System Details
  - Windows 2003 Server
    - IIS 6.0 (16 Systems) – Behind On Vendor Updates
  - Windows 2008 Server
    - IIS 7.0 (12 Systems)
- Remote Access For Physicians/Support
  - Remote Desktop Web Access Through Browser
  - Terminal Services Clients
- HIPAA Compliant RDP Crypto Access?

Case Study – Fetal Monitors

- FDA MAUDE Reports
  - Several Cases Of Fetal Alarm Capability Disabled
- Is There Correlation To Exposed Devices?
  - Impossible To Tell From MAUDE Alone
    - User Submitted Reports
    - Sanitized Data
    - Attachments Removed
- BTW - MAUDE Reports And Search Interface Are “Teh Suck”

Case Study – Fetal Monitors

- So Where Are We Today?
  - I Previously Disclosed This To DHS In Fall 2012
  - Many Still On Public IP
  - Several Still Running IIS 6.0
- Vendor Did Reach Out
  - Conference Call, Interest In Customer Misuse Cases, Security Researcher Communication
- Lessons Learned
  - Need Better Reporting Method
  - Need Follow-Up Action
  - Need Authority For Location Identification

Adversary Misconceptions

- Adversaries Only Care About Financial Gain
  - OK Maybe The Russians Do!!
- Adversaries Live In Caves & Can't Figure It Out
  - I Swear Some Ignorant Individual Actually Emailed Me This.
- Adversaries Are Not Technically Adept To Carry Out An Attack On Medical Devices
  - Everything We Just Showed You Requires Little Skill To Execute. Basic Security Concepts. Open Source Reconnaissance & Publicly Disclosed Vulnerabilities.

Adversaries We Should Worry About

- Terrorists/Extremists
  - Especially Technically Adept & Active Adversaries Like ISIS.
- Nation State
  - State Sponsored Actors
- Patients Themselves
  - Patients Downloaded Documentation, Retrieved Service Technician Login And Changed Infusion Pump Dosage
    - http://austriantimes.at/news/General_News/2012-12-01/45780/Patient_hackers_managed_to_dial_a_drug_in_hospital

Adversary Attack Model

- Greatest Risk Is A Combined Attack
  - Event Such As Boston Marathon Bombing Or 9/11 In Conjunction With Attacking Healthcare System Or Power Plant, etc..
- Really Is That A Risk?
  - Our Government Thinks So. You Probably Should Listen.
- CyberCity – Ed Skoudis/Counter Hack
  - http://www.washingtonpost.com/investigations/cybercity-allows-government-hackers-to-train-for-attacks/2012/11/26/588f4dae-1244-11e2-be82-c3411b7680a9_story.html

Has An Attack Already Happened?

- How Would You Know If A Medical Device Was Hacked?
  - Closed Source Code
  - Specialized Diagnostic Equipment, Proprietary Protocols
- Lack Of Forensic Capabilities In Medical Devices
  - Lack Of Medical Device Forensic Experts
  - Only 2 On Linked-In, FDA & Ret. FBI
  - FDA Only Adjudicates Devices For Generic “Malfunction”
- How Do You Prove An Attack Or Adverse Event Without Evidence Or Audit Log Trail?

Doesn't HIPAA Protect Us? It Must Be Ineffective

- Yes I Get These Emails As Well!! I Won't Argue The Ineffectiveness!!
- HIPAA Focuses On Privacy Of Patient Data
- HIPAA Does Not Focus On Medical Device Security
- HIPAA Does Not Focus On Adversary Resilience Testing And Mitigation

Doesn't FDA, DHS, FBI, HHS, etc.. Protect Us?

- No. It's Your Responsibility To Secure Your Environment.

- They Have Told You With Recent Advisories To Start Testing These Devices And Assessing Risk.

- **ICS-ALERT-13-164-01**
- **FDA UCM356423**
- **FBI PIN # 140408-009**

What Caused These Issues In Healthcare?

- HIPAA Drives Information Security Program & Budget
- Security Is Not Compliance/Information Assurance
- Check Box Security Is Not Effective
- Policy Does Not Prevent Adversarial Risks

What Caused Issues In Manufacturers?

- Never Had To Design For Adversarial Threats
- Just Starting To Build Information Security Teams
- Historically Focused On Regulatory Compliance Just Like Healthcare
- Haven’t Fully Embraced Partnering With Security Researchers

Common Disconnects With Manufacturers

- Been Told They Can't Patch/Update Systems
  - http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm077812.htm
- Been Told They Can't Change Hard-Coded Admin (Support) Accounts
- Biomed – IS/Information Security Integration
- Know Your Manufacturer's Information Security Employees – Maintain Relationship

Patching Questions

- Yes You Can…But Should You?
- Complex Ecosystem Of Medical Devices
  - Leased, 3rd Party Managed, Multi-Vendor
- What If Patch Breaks Medical Device Or Results In Patient Safety Issue?
  - Liability
- Many Healthcare Organizations Reluctant To Patch Or Modify Medical Devices

Anti-Virus Questions

- Several FDA MAUDE Reports Of Negative Impact
- McAfee DAT 5958 on 21 April, 2010
  - Svschost.exe Flagged As Wecorl-A Resulted In Continuous Reboot Of Systems
  - 1/3rd Of Hospitals In Rhode Island Impacted
- AV Deleted Fetal Monitor Logs (7 Hours)
  - http://hosted.verticalresponse.com/250140/86af97f052/

Solutions & Recommendations

- External Attack Surface Reduction & Hardening
- Recognize & Mitigate Your Exposure To Tools Like Shodan
  - Shodan API = Automation
  - Needs Continual Monitoring, Roll Your Own
  - Other Fast Scanning Tools: Masscan, ZMAP
- Make Your External Perimeter Metasploit Proof
  - Yes You Actually Have To Use Metasploit

Solutions & Recommendations

- Stop The Bleeding
  - Remove SMB Services
- Adversarial Resilience Testing
  - Red Teaming
  - Harden Edge Devices To Applicable NIST Standards

Needs From Healthcare Industry

- Internal programs focused on medical device security to include device security testing
- Require security testing during vendor selection and procurement process
- Work to show organization you are supporting their mission and values

Needs From Healthcare Industry

- Request MDS2 Forms From Vendors
  - Incorporate Into Contract With Penalties
- Responsibly Disclose Findings To Manufacturer, FDA, DHS/ICS-CERT
  - Possibly HHS OCR, FBI, FTC
- Demand Vulnerabilities Are Remediated
  - Incorporate Into Contract With Penalties
  - Incorporate Indemnification Clauses Into Contract

Recommended Disclosure Reporting

- Individual Researchers
  - DHS/ICS-CERT
  - FDA
  - Manufacturer – If Possible
  - CVE, OSVDB If Appropriate
- Healthcare Organizations
  - Manufacturer
  - DHS/ICS-CERT
  - FDA
  - CVE, OSVDB If Appropriate

Accessibility Of Medical Devices

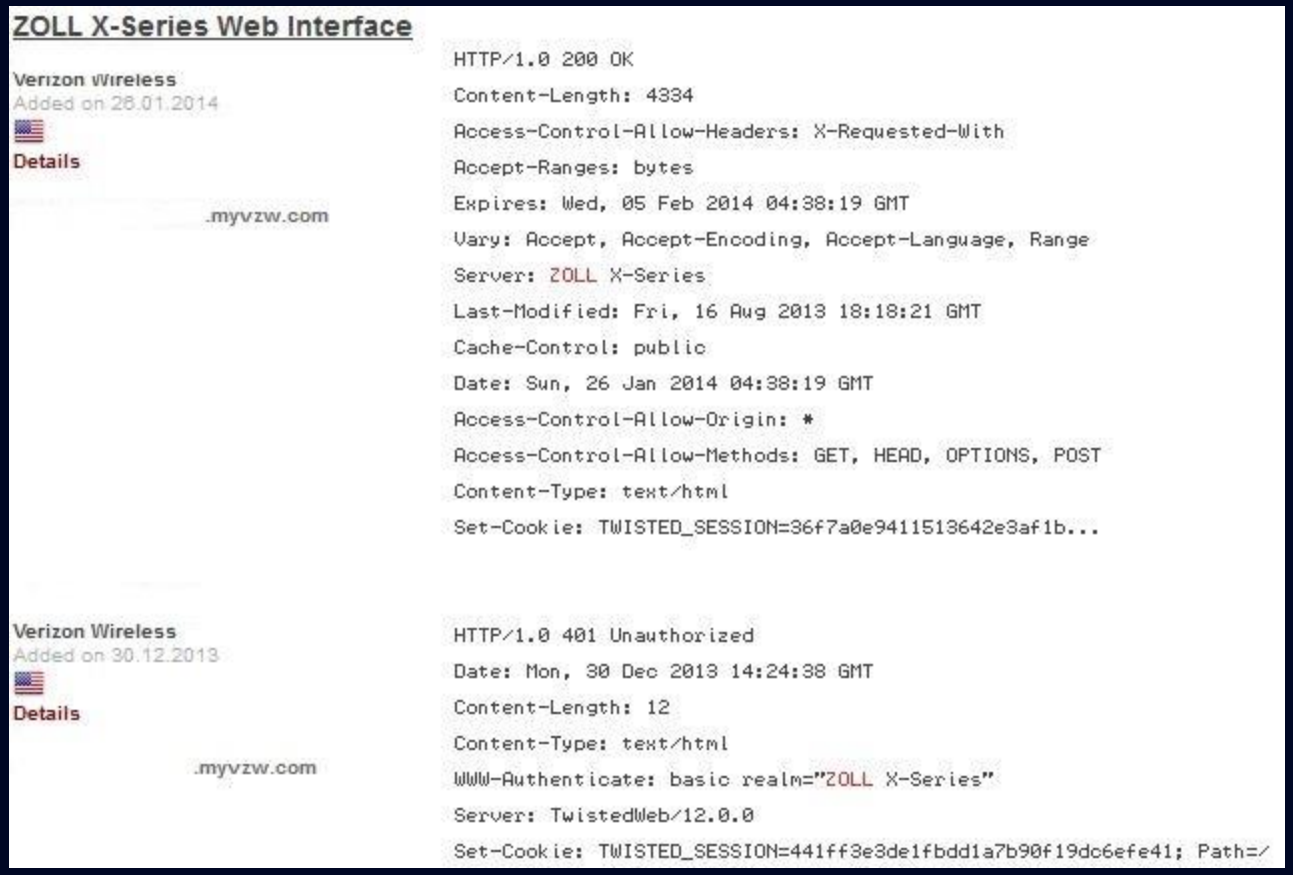
- Difficult To Get Hands On Medical Devices
  - Many Devices Are Rx Only
  - Many Devices Are Very Expensive
- Independent Research Options
  - Ebay or MEDWOW (Can Be End-Of-Life, Recalled)
  - Hack Your Own Device
- Consultant
  - Most Often End Up Under NDA
  - Starting To See Non-Identifiable Data Clauses

Do You Really Need The Medical Device?

- Use Search Engines To Locate Service Manuals
  - Contain Detailed Systems & Operations Information
  - Contain Support Or Service Technician Login Information
  - Contain Detailed Architecture & Schematics

Case Study – Defibrillators

- Located Zoll X Series Defibrillators On Public IP Space

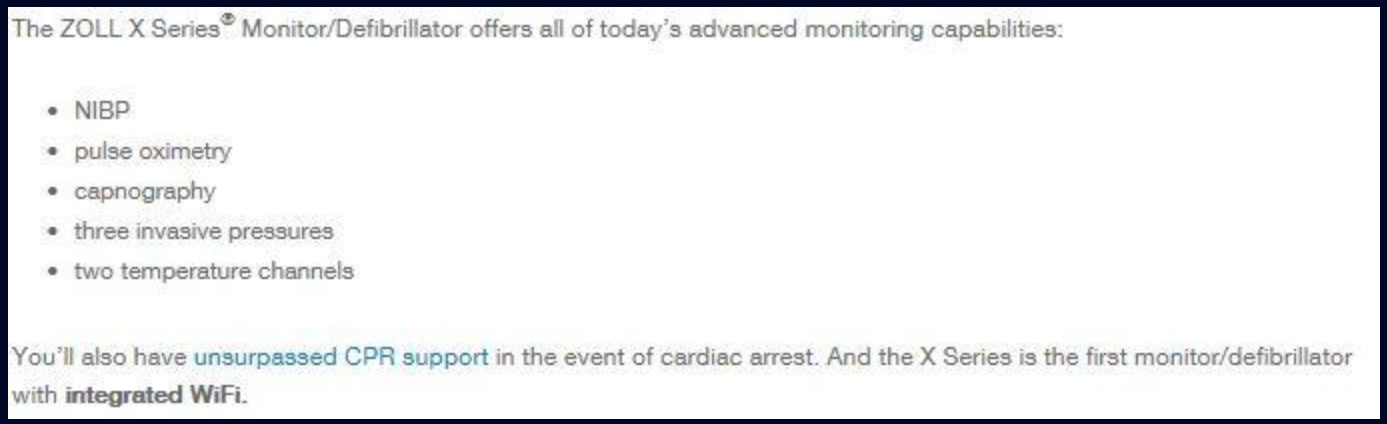


Case Study – Defibrillators

- You Need A Certificate For Web Interface.
  - Thank God It's On The Landing Page!!!!

Case Study – Defibrillators

- Defibrillator Also Is First To Market With Integrated Wireless & Bluetooth Interfaces
  - By Design Of Course



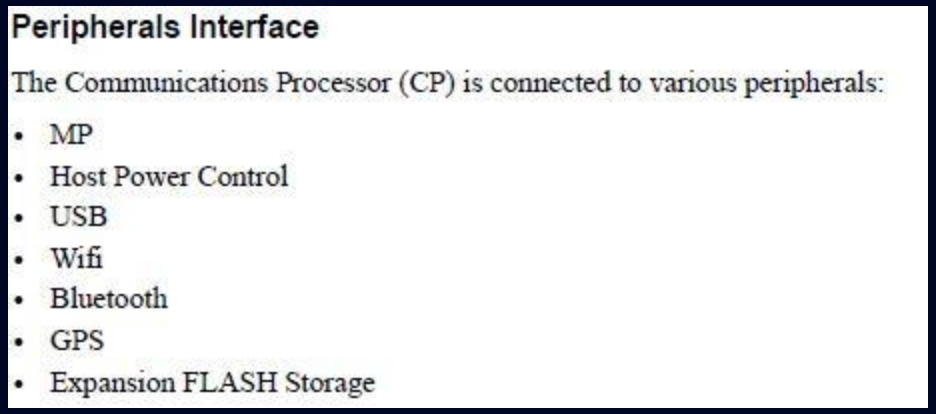
The ZOLL X Series® Monitor/Defibrillator offers all of today's advanced monitoring capabilities:

- NIBP
- pulse oximetry
- capnography
- three invasive pressures
- two temperature channels

You'll also have unsurpassed CPR support in the event of cardiac arrest. And the X Series is the first monitor/defibrillator with **integrated WiFi**.

Case Study – Defibrillators

- Wireless & Bluetooth Interfaces Also Have Direct Access To Communications Processor
  - Utilizes UART Interface



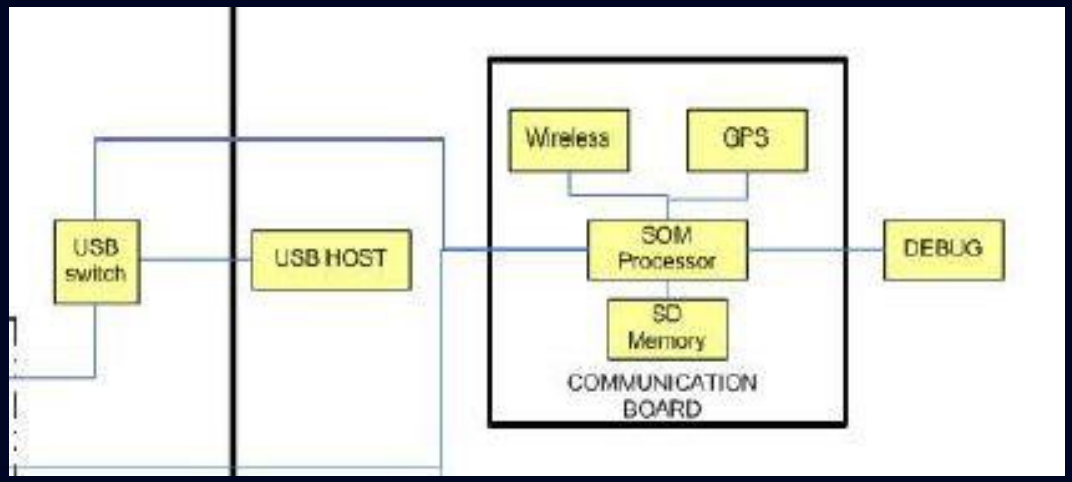
Peripherals Interface

The Communications Processor (CP) is connected to various peripherals:

- MP
- Host Power Control
- USB
- Wifi
- Bluetooth
- GPS
- Expansion FLASH Storage

Case Study – Defibrillators

- Communications Processor Must Be Separated Completely From Main Monitor Board Right?
  - Debug Is Located On GPS UART On CP
  - Schematics Show Communication Back To Main Monitor Board As Well
  - Note USB On Same Circuit Back To Main Board



Case Study – Defibrillators

- In Order To Import Configuration You Utilize USB With A File Named ZollConfig.xml

Importing Configuration Information from USB

Importing a configuration file imports the system and patient setup information from a file named ZollConfig.xml on the USB device.

Note: Make sure the file you are importing is named ZollConfig.xml. Otherwise, the import will not work.

Case Study – Defibrillators

- Critical Configuration Values

Note: Review critical configuration values such as alarm, AED, defibrillator, and pacer settings to verify that you imported the correct configuration file.

- Alarm Parameters

Trend on Alarm

The Trend on Alarm parameter allows you to specify whether or not to log Trends each time an alarm occurs.

The values for the Trend on Alarm parameter are:

Possible Values:	On, Off
Default:	Off

Case Study – Defibrillators

- Default Patient Mode

Default Patient Mode

The Default Patient Mode parameter allows you to specify the default age group of the patients using the X Series unit.

The values for the Default Patient Mode parameter are:

Possible Values:	Adult, Pediatric, Neonate
Default:	Adult

- Factory Reset

Restoring Factory Default Configuration Settings

You can restore all the current configuration settings to their factory default settings. However, if the language is different than the default setting, it will not change.

Note: You must have authorized supervisor access to restore the factory default settings.

Case Study – Defibrillators

- Supervisor Access

Accessing the Supervisor Menu

To access the Supervisor menu, press the More () and Setup () quick access keys, and select **Supervisor**. You are then required to enter the four digit Supervisor passcode before accessing the configurable options in the menus.

- Supervisor Mode Config Settings

The Supervisor menu includes the following parameter settings.

- "Alarms Parameters" on page 52
- "Log Parameters" on page 104
- "Defib/Pacer Parameters" on page 108
- "ECG Parameters" on page 110
- "NIBP Parameters" on page 112
- "Printer Parameters" on page 114
- "Display/Configuration Parameters" on page 116
- "AED/Advisory Parameters" on page 126
- "CPR Parameters" on page 132
- "Communications Parameters" on page 136
- "Service Parameters" on page 138

Case Study – Defibrillators

- Supervisor Default Login

Note: The X Series unit ships from ZOLL with both the default supervisor passcode and the service passcode set to 1234.

- Clearing Logs

Log Clear Restriction

If you set this parameter to **User confirmation** the user will be prompted with a confirmation dialog before clearing the disclosure log. If you set this parameter to **Passcode** the user will have to enter a passcode and then be prompted with a confirmation dialog before clearing the disclosure log.

The values for the Log Clear Restriction parameter are:

Possible Values:	User confirmation, Passcode
Default:	User confirmation

Log Clear Code

The values for the Log Clear Code parameter are:

Possible Values:	Numeric
Default:	1234

Case Study – Defibrillators

- So Who Thinks This Is A Secure Design?
- So Is This A Problem In Only One Product Line?
  - Of Course Not

Case Study – Defibrillators

- Zoll M Series Defibrillator
  - System Config – 00000000
- Zoll R Series Defibrillator/Monitor
  - System Config – 00000000
- Zoll E Series Defibrillator/Monitor
  - System Config – 00000000
- Zoll X Series Defibrillator/Monitor
  - Supervisor Passcode – 1234
  - Service Passcode - 1234

How Are Vendors Changing?

- They Have Started Talking To Researchers
- Owlet Baby Care – Huge Shout Out!!
  - Stepped Up And Is Letting Us Test Security Of Device Prior To Market
  - Recognizes Patient Safety Concerns Due To Security Vulnerabilities
- Philips Healthcare Released Responsible Disclosure Positioning

Philips Healthcare Responsible Disclosure Positioning

Product Security & Services Office
Philips Healthcare
August 2014

PHILIPS

Philips Healthcare Responsible Disclosure Positioning

- **Philips Healthcare and Responsible Disclosure**
- Philips Healthcare recognizes the need for clear a Responsible Disclosure Policy and protocols as part of its Product Security function.
- The company is developing a Responsible Disclosure Policy according to current industry best practices.
  - The policy will be publicly accessible, with clear communications channels for customers, researchers and other security community stakeholders.
  - The policy will be based on principles of transparency, accountability and responsiveness.
  - The policy will outline defined protocols for reporting and response, managed by the Philips Product Security Team.
    - The policy protocols will encompass:
      - Monitoring and response of inbound communications
      - Managing confirmation receipt and follow-up communication with senders
      - Evaluation of vulnerability notifications and status tracking
      - Alignment with incident response, stakeholder notification, remediation and prevention protocols as required
- Philips has actively sought out researcher and analyst input to help guide policy design and projected implementation.
  - The company has increasingly engaged with the security research community over the past year.
  - Philips is committed to ongoing dialogue with the security community and to productive partnerships.

PHILIPS

How To Help?

- Looking For Android/iOS Security Researchers To Collaborate On Healthcare Application Security
- Seeking Collaboration With Physicians & Patients

Gr33tz

- Barnaby Jack

- John Matherly
- Terry McCorkle
- Jay Radcliffe
- Billy Rios

- DHS/ICS-CERT
- FDA/HHS/CDRH
- FBI

Roche Diagnostics
Philips Healthcare

Contact Info

- Scott Erven
  - @scotterven
  - @secmedic
  - scott@secmedic.com
- Shawn Merdinger
  - @medseclinkedin
  - shawnmer@gmail.com